Diffieho-Hellmanova výměna klíčů

- Veřejné parametry: prvočíslo p, generátor g grupy $\mathbb{Z}_p^*$
- Alice vygeneruje $x \in \{0 - p-2\}$ a pošle Bobovi $g^x \pmod p$
  Bob —"— $y \in \{0 - p-2\}$ —"— Alici $g^y \pmod p$
  ⇒ oba umí spočítat $g^{xy} = (g^x)^y = (g^y)^x$,
  ale Eva nikoli (leda by uměla počítat diskrétní log) ← nicméně tohle není ekvivalence
- Pozor, aktivní útočník může vstoupit do komunikace a nechat každou stranu, ať si bezpečně vymění klíč s ním (pak přeposílá zprávy)
  ⇒ nutno podepisovat! Typicky: pomocí RSA podepíši hash vygenerovaného klíče (v obou směrech)
- Pokud se strany na parametrech p, g dohadují (nebo nevěříme tomu, kdo je stanovil), musíme kontrolovat, že p je prvoč. a g generátor (obojí už umíme)
  → jinak útočník zvolí g, které generuje dost malou podgrupu, aby v ní uměl logaritmovat 😊
- Podobně by aktivní útočník mohl najít k takové, aby g^k generovalo malou podgrupu, a pak vyměnit g^x za $(g^x)^k$ a podobně g^y za $(g^y)^k$ ⇒ tím Alici i Boba zahnal do podgrupy.
  (A oni by pak spokojeně podepsali vygenerovaný klíč...
  lépe: podepisovat celý průběh protokolu)
- DH prozrazuje 1 bit: z $\left(\frac{g^x}{p}\right)$ se pozná lichost x, podobně lichost y
  ⇒ umíme poznat $\left(\frac{g^{xy}}{p}\right)$, tedy zda protokol vygeneruje QR.
- $\mathbb{Z}_p^*$ má určitě 2 podgrupy: $\underbrace{\{-1, 1\}}_{\text{řádu } 2}$ a $\underbrace{QR}_{\text{řádu } \frac{p-1}{2}}$.

  Pokud $\frac{p-1}{2}$ je prvočíslo (tedy $p = 2q+1$), pak už žádné jiné.
  ⇒ nikdo nás do nich nezavede.

  A pokud se budeme pohybovat v podgrupě QR, už nebudeme ani vyzrazovat informace.
  ⇒ místo generátoru tedy použijeme g^2 + testujeme, zda g^x, g^y leží v podgrupě.

- Abychom se vyhnuli velkým exponentům...
  Zvolíme $p = kq+1$, kde q má cca 256b, p výrazně více.
  Pracujeme v podgrupě generované g^k, ta má q prvků.
  ⇒ Opět kontrolujeme, zda se držíme v těle podgrupě ($a^q = 1$)
  a opět nás nikdo nemůže zahnat do menší.
- Obecně: DH funguje v grupách, v nichž je dlog těžký a které nemají netriviální podgrupy
- $p = 2q+1$ je obecně bezpečné ($p-1$ nesmí mít samé malé faktory, jinak umíme dlog)
- Sémantická bezpečnost: zjistit nejnižší bit je stejně těžké jako získat celé číslo (podobně jako RSA)
- DH jako asymetrická šifra: veřejný klíč je g^x, tajný x.

ElGamalův kryptosystém – asym. šifra založená na dlog

Parametry: prvočíslo p, generátor g grupy $\mathbb{Z}_p^*$

Klíče: $k \in_R \{0 \dots p-2\}$ → tajný klíč k
$h = g^k \bmod p$ veřejný klíč h

Šifrování: $t \in_R \{0 \dots p-2\}$
$s = h^t \ (= g^{kt})$
$y = x \cdot s$
→ pošleme zprávu (g^t, y)

tohle je vlastně DH: 1. krok při generování klíče, 2. krok při šifrování. Tím vymícháme s a pak jím zašifrujeme x.

Dešifrování: $s = (g^t)^k$ ... rekonstruujeme sdílené tajemství s
$x = y \cdot s^{-1}$ ... pomocí s dešifrujeme

! randomizace je kritická, jinak z known plaintextu spočítáme s !

Podobně jako RSA prosakuje, zda x je QR
... ale to jde snadno napravit vybíráním zpráv jen z množiny QR

Na rozdíl od RSA musí být šifr. klíč veřejný a dešifr. tajný, protože z dešifr. umíme vždy odvodit šifr.

Obecně: ElG. lze provozovat v jakékoliv grupě, v níž je dlog těžký (podobně jako DH)

---

pomocí veřej. klíče:

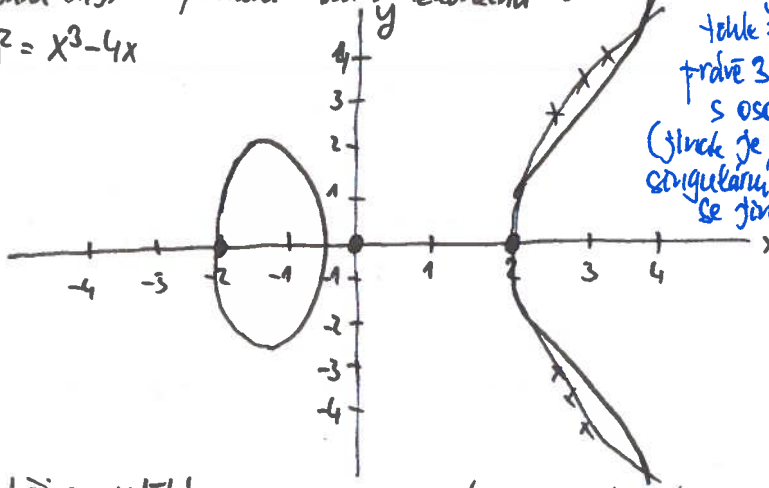
① pokud k je sudé:
$\left(\frac{h}{p}\right) = \left(\frac{g^k}{p}\right) = (-1)^k = 1$
$\Rightarrow \left(\frac{yh^t}{p}\right) = 1 \Rightarrow \left(\frac{x}{p}\right) = \left(\frac{y}{p}\right)$

② pokud k je liché:
$\left(\frac{h}{p}\right) = -1$
$\left(\frac{s}{p}\right) = \left(\frac{h^t}{p}\right) = (-1)^t = \left(\frac{g^t}{p}\right)$
$\Rightarrow \left(\frac{y}{p}\right) = \left(\frac{x}{p}\right) \cdot \left(\frac{g^t}{p}\right)$

Eliptické křivky – dobrý zdroj malých grup s těžkým dlogem

- Nad reálnými čísly: uvažme množinu všech $(x,y) \in \mathbb{R}^2$ t.ž.
  $y^2 = x^3 + ax + b$ (kde a,b jsou param. t.ž. $4a^3+27b^2 \neq 0$)
  $E :=$ všechna (x,y) + speciální "bod v nekonečnu" $\mathcal{O}$

- Příklad: $y^2 = x^3 - 4x$



tohle zaručuje právě 3 průsečíky s osou x (jinak je křivka singulární a chová se jinak)

- 2 bodů na křivce udělám grupu s operací + a neutrálním prvkem $\mathcal{O}$
  Jak vypadá $P+Q$ pro $P=(x_1,y_1)$ a $Q=(x_2,y_2)$:
  1. $x_1 \neq x_2$: uvažme přímku PQ. Ta křivku protne ve 3 bodech: P, Q, R. Za výsledek prohlásíme zrcadlový obraz bodu R podle osy x.
  2. $x_1 = x_2$, $y_1 = -y_2$: výsledek je $\mathcal{O}$
  3. $x_1 = x_2$, $y_1 = y_2$: podobně jako 1, ale přímka bude tečna v bodě $P=Q$.

  Triviální: $P+Q = P-Q$, $P + (-P) = \mathcal{O}$ (přehlopení znaménka y)

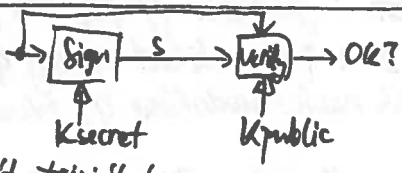
  Netriviální: $+$ je asociativní (lze dokázat pracně mechanicky nebo vybudovat hlubokou teorii)

- Totéž můžeme budovat nad konečným tělesem mod p, $p>3$ (nebo $\mathbb{F}_{p^k}$ pro $p>3$)
  [pozn.: jsme tytéž formule pro definici $+,-$]
  → zase vznikne abelovská grupa (komutativní)

- Věta [Hasse]: Je-li E el. křivka nad tělesem $\mathbb{F}_q$, pak: $q+1-2\sqrt{q} \leq |E| \leq q+1+2\sqrt{q}$.
  → existuje Schoofův alg., který $|E|$ spočte přesně v poly čase.
  [pro $p=2,3$ to funguje trochu jinak]

- **Věta:** Je-li $(E,+)$ eliptická křivka nad $\mathbb{F}_q$, pak $\exists n_1, n_2$:
  $(E,+) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, přičemž $n_2 \mid n_1$.
  → pokud $|E|$ je prvočíslo nebo součin různých prvočísel, pak $n_2 = 1$, takže $(E,+)$ je cyklická grupa ⇒ funguje v ní DH.
  → jinak můžeme najít cykl. podgrupu velikosti n_1.
- **Komprese bodů:** místo páru (x,y) stačí přenést x + 1 bit, který vybere jednu z možných druhých odmocnin (1 je sudá, druhá lichá ⇒ stačí nejnižší bit)
- **eliptický ElGamal:** DH na křivce, pak hešovací fce z křivky do $\mathbb{Z}_p$, kde provedeme maskování zprávy.
- **bezpečné křivky** (s těžkým dlog) není snadné sehnat: na mnoho typů křivek existují efektivní algoritmy na dlog?
  → https://safecurves.cr.yp.to/

Asymetrické podpisy



- Sign může využívat náhodu ⇒ verify nemusí být triviální
- **Cíle útočníka:**
  - zjištění tajného klíče
  - existenční padělání (vytvoří podpis nějaké nové zprávy)
  - cílené padělání (podpis předem určené zprávy)
- **Možnosti útočníka:**
  - zná veřejný klíč
  - zná podpisy nějakých zpráv
  - může si nechat podepsat, cokoli bude chtít různé od zadaných ↑

- **podpisy pomocí RSA:** tajný e, veřejný d, $sig = x^e \bmod n$.
  - exist. padělání na základě veř. klíče: vyberu si sig, pak $x := sig^d \bmod n$. (to je nejspíš nesmyslná zpráva)
  - ze slepých podpisů plyne cílené padělání při CPA.
  - **oprava:** zprávu před podepsáním hešuji.